

Appl. No. 10/005,972  
Response Dated January 19, 2006  
Reply to Final Office Action of October 19, 2005

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application.

**Listing of Claims:**

1. (Currently Amended) A method to manage secure connections, comprising:  
receiving an encrypted packet having an a security identifier and an external address that represents a plurality of internal addresses;  
translating said external address by selecting one of said internal addresses associated with said security identifier using a list of security identifiers and a set of heuristics; and  
communicating said encrypted packet to said selected internal address.
2. (Currently Amended) The method of claim 1, wherein said selecting comprises further comprising:  
searching a list of security identifiers having associated times;  
selecting an a security identifier having an earliest time; and  
retrieving said internal address associated with said selected security identifier.
3. (Original) The method of claim 2, wherein said searching comprises further comprising:  
creating said list; and

Appl. No. 10/005,972  
Response Dated January 19, 2006  
Reply to Final Office Action of October 19, 2005

searching said created list.

4. (Currently Amended) The method of claim 3, wherein said creating comprises:  
receiving an encrypted packet having a predetermined sequence number and ~~an a~~  
security identifier from a device associated with one of said internal addresses;  
determining a time said encrypted packet was received;  
associating said time and said internal address with said security identifier; and  
storing said security identifier with said associated time and associated internal  
address.
5. (Original) The method of claim 1, wherein said packet is encrypted in accordance  
with the Internet Security Association And Key Management Protocol (ISAKMP).
6. (Original) The method of claim 1, wherein said encrypted packet is an Internet  
Protocol (IP) Encapsulating Security Payload (ESP) encrypted packet.
7. (Currently Amended) The method of claim 1, wherein said security identifier is a  
security parameter index (SPI).
8. (Currently Amended) The method of claim 1, wherein said security identifier  
represents a tunnel between two devices, and further comprising:  
receiving a message that said encrypted packet was communicated to an incorrect  
internal address;

Appl. No. 10/005,972  
Response Dated January 19, 2006  
Reply to Final Office Action of October 19, 2005

determining activity levels for each tunnel terminating at each device represented by said plurality of internal addresses; and  
communicating said encrypted packet to an internal address having a tunnel with a highest activity level.

9. (Currently Amended) A method to manage secure connections, comprising:  
creating a list of security identifiers, with each security identifier representing a tunnel terminating at a device having an internal address;  
translating each of said internal addresses to an external address;  
receiving an encrypted packet having said external address;  
translating said external address by selecting one of said internal addresses associated with a security identifier from using said list of security identifiers using and a set of heuristics; and  
communicating said encrypted packet to said selected internal address.
10. (Original) The method of claim 9, wherein said tunnel is created in accordance with the Internet Security Association And Key Management Protocol (ISAKMP).
11. (Original) The method of claim 9, wherein said encrypted packet is an Internet Protocol (IP) Encapsulating Security Payload (ESP) encrypted packet.
12. (Currently Amended) The method of claim 9, wherein said security identifier is a security parameter index (SPI).

Appl. No. 10/005,972  
Response Dated January 19, 2006  
Reply to Final Office Action of October 19, 2005

13. (Currently Amended) The method of claim 9, wherein said selecting comprises further comprising:

searching said list of security identifiers having associated times;  
selecting ~~an~~ a security identifier having an earliest time; and  
retrieving said internal address associated with said selected identifier.

14. (Currently Amended) The method of claim 9, wherein said creating comprises:

receiving an encrypted packet having ~~an~~ a security identifier from a device associated with one of said internal addresses;  
determining a time said encrypted packet was received;  
associating said time and said internal address with said security identifier; and  
storing said security identifier with said associated time and internal destination address.

15. (Currently Amended) A secure connection manager, comprising:

a flow module to create a list of security identifiers, with each security identifier representing a secure flow terminating at a device with an internal address; and  
a translation module to select an internal address for an encrypted packet having an external address and a ~~flow~~ security identifier using said list of security identifiers and a set of heuristics.

Appl. No. 10/005,972  
Response Dated January 19, 2006  
Reply to Final Office Action of October 19, 2005

16. (Original) The secure connection manager of claim 15, further comprising:  
a communication module to communicate said encrypted packet to said selected internal address.
17. (Currently Amended) A system to manage secure connections, comprising:  
a first network node to send encrypted packets to an external address;  
a second network node to receive said encrypted packets and translate said external address to an internal address using a list of security identifiers and a set of heuristics; and  
a third network node having said internal address to receive said encrypted packets.
18. (Original) The system of claim 17, wherein said second network node is a router configured to perform natural address translation (NAT).
19. (Original) The system of claim 17, wherein said first and third network nodes are configured to communicate using a tunnel created in accordance with the Internet Security Association And Key Management Protocol (ISAKMP).
20. (Original) The system of claim 17, wherein said encrypted packets are Internet Protocol (IP) Encapsulating Security Payload (ESP) encrypted packets.

Appl. No. 10/005,972  
Response Dated January 19, 2006  
Reply to Final Office Action of October 19, 2005

21. (Original) The system of claim 17, wherein said second network node performs said translation using a list of flow identifiers, with each flow identifier representing a security parameter index (SPI) and having an associated internal address and receipt time.

22. (Currently Amended) An article comprising:

a storage medium;

said storage medium including stored instructions that, when executed by a processor, result in managing a secure connection by receiving an encrypted packet having ~~an~~ a security identifier and ~~an~~ external address that represents a plurality of internal addresses, translating said external address by selecting one of said internal addresses associated with said security identifier using a list of security identifiers and a set of heuristics, and communicating said encrypted packet to said selected internal address.

23. (Currently Amended) The article of claim 22, wherein the stored instructions, when executed by a processor, further result in selecting one of said internal addresses by searching a list of security identifiers having associated times, selecting ~~an~~ a security identifier having an earliest time, and retrieving said internal address associated with said selected security identifier.

24. (Currently Amended) The article of claim 23, wherein the stored instructions, when executed by a processor, further result in searching said list of security identifiers by creating said list, and searching said created list.

Appl. No. 10/005,972  
Response Dated January 19, 2006  
Reply to Final Office Action of October 19, 2005

25. (Currently Amended) The article of claim 24, wherein the stored instructions, when executed by a processor, further result in creating said list by receiving an encrypted packet having a predetermined sequence number and ~~an~~ a security identifier from a device associated with one of said internal addresses, determining a time said encrypted packet was received, associating said time and said internal address with said security identifier, and storing said security identifier with said associated time and associated internal address.

26. (Currently Amended) An article comprising:  
a storage medium;  
said storage medium including stored instructions that, when executed by a processor, result in managing secure connections by creating a list of security identifiers, with each security identifier representing a tunnel terminating at a device having an internal address, translating each of said internal addresses to an external address, receiving an encrypted packet having said external address, translating said external address by selecting one of said internal addresses associated with a security identifier from using said list of security identifiers using and a set of heuristics, and communicating said encrypted packet to said selected internal address.

27. (Currently Amended) The article of claim 26, wherein the stored instructions, when executed by a processor, further result in selecting one of said internal addresses by searching said list of security identifiers having associated times, selecting ~~an~~ a security

Appl. No. 10/005,972  
Response Dated January 19, 2006  
Reply to Final Office Action of October 19, 2005

identifier having an earliest time, and retrieving said internal address associated with said selected security identifier.

28. (Currently Amended) The article of claim 26, wherein the stored instructions, when executed by a processor, further result in creating said list of security identifiers by receiving an encrypted packet having ~~an~~ a security identifier from a device associated with one of said internal addresses, determining a time said encrypted packet was received, associating said time and said internal address with said security identifier, and storing said security identifier with said associated time and internal destination address.